

# Coefficient Extraction Formula and Furstenberg's Theorems

YINING HU

CNRS, Institut de Mathématiques de Jussieu-PRG

Université Pierre et Marie Curie, Case 247

4 Place Jussieu

F-75252 Paris Cedex 05 (France)

yining.hu@imj-prg.fr

## Abstract

In this article, using a Proposition of Furstenberg, we give a coefficient extraction formula for algebraic series that is valid for all fields, of which the Flajolet-Soria coefficient extraction formula for the complex field is a special case.

## 1 Introduction

Combinatorists often use the “Flajolet-Soria” formula, first published in [10], that gives an explicit expression for the coefficients of an algebraic power series. Our main theorem is that (a generalization of) this result can be deduced from a theorem of Furstenberg going back to 1967 [6, Proposition 2].

In the paper of Furstenberg, a useful notion for the study of multiple variable formal power series is their diagonals. For the formal power series in  $\kappa((x_1, \dots, x_m))$

$$f(x_1, x_2, \dots, x_m) = \sum_{n_i > -\mu} a_{n_1 n_2 \dots n_m} x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}$$

its (principal) diagonal  $\mathcal{D}f(t)$  is defined as the element in  $\kappa((t))$

$$\mathcal{D}f(t) = \sum a_{nn\dots n} t^n.$$

Furstenberg [6] proved the following results:

**Theorem 1.** (Furstenberg) *Let  $\kappa$  be a field of positive characteristic. Let  $f(x_1, \dots, x_m)$  be an element of  $\kappa((x_1, \dots, x_m)) \cap \kappa(x_1, \dots, x_m)$ , that is,  $f$  is a formal power series of several variables that represents a rational function. Then  $\mathcal{D}f(t)$ , the diagonal of  $f$ , is algebraic over  $\kappa(t)$ .*

**Proposition 1.** (Furstenberg) *Let  $P(X, Y)$  be a polynomial and  $\varphi(X) = \sum_1^\infty c_n X^n$  a formal power series in  $\kappa((X))$  satisfying  $P(X, \varphi(X)) = 0$ . If  $(\partial P / \partial Y)(0, 0) \neq 0$ , then*

$$\varphi = \mathcal{D}\{Y^2 \frac{\partial P}{\partial Y}(XY, Y) / P(XY, Y)\}.$$

Here  $\kappa$  is an arbitrary field.

**Theorem 2.** (Furstenberg) *Let  $\mathbb{F}_q$  be a finite field of characteristic  $p$ . If a formal power series  $\phi(X) \in \mathbb{F}_q((X))$  is algebraic over  $\mathbb{F}_q(X)$ , then  $\phi = \mathcal{D}(R(X, Y))$  for a formal power series in two variables  $R(X, Y) \in \mathbb{F}_q(X, Y)$  that represents a rational function of  $X$  and  $Y$ .*

On the other hand, on a finite field, the formal power series algebraic over the field of rational fractions are characterized by a simple combinatorial property:

**Theorem 3.** (Christol) *Let  $\mathbb{F}_q$  be a finite field of characteristic  $p$ . A formal power series*

$$f = \sum_{n=0}^{\infty} u_n X^n \in \mathbb{F}_q[[X]]$$

*is algebraic over the rational function field  $\mathbb{F}_q(X)$  if and only if the  $p$ -kernel of  $u$*

$$\{(u_{n \cdot p^k + r})_n \mid k \in \mathbb{N}, r = 0, 1, \dots, p^k - 1\}$$

*is finite.*

These notions are revisited in this article. In Section 2, it is proved that the Flajolet-Soria [10] formula for coefficients of algebraic series over  $\mathbb{C}(X)$  is a consequence of Proposition 1 of Furstenberg, with which we can obtain a similar formula that can be applied to all fields. In Section 3, a simple proof of Theorem 1 of Furstenberg is given using a generalization of Christol's Theorem. On the other hand, Theorem 2 of Furstenberg gives another proof of one direction of Christol's Theorem. In Section 4, in order to construct a rational function whose diagonal is a given algebraic function, an algorithm is given, which calculates an annihilating polynomial of an algebraic function. Finally a method of finding (in  $\mathbb{F}_q[[X]]$ ) roots of polynomials in  $\mathbb{F}_q(X)[Y]$  using automata is illustrated with examples.

Among several papers related to diagonals of multivariate formal power series, we would like to cite two recent works: a paper by Adamczewski and Bell [1] about a quantitative version of the theorem of Furstenberg, and the doctoral thesis of Lairez that gives, in particular, an interesting characterization of binomial sums in terms of diagonals [7, Ch. III].

## 2 Coefficients of an algebraic series

There is a link between combinatorial objects and power series in  $\mathbb{C}$ . The study of generating functions using the tools of complex analysis gives us information about a combinatorial structure. The following theorem from [10] (see also [2] and [9]) allows us to extract the coefficients of an algebraic series in  $\mathbb{C}$  from an annihilating polynomial of it. For more reference on the formula, one can look at the article by Banderier and Drmota[2].

For an element  $A$  in  $\mathbb{F}_q((X, Y))$   $A = \sum_{m,n} a_{m,n} X^m Y^n$ , we let  $[X^m Y^n]A$  denote the coefficient  $a_{m,n}$ .

**Theorem 4.** (The Flajolet-Soria formula for coefficients of algebraic series) *Let  $P(X, Y)$  be a polynomial over the complex field such that  $P(0, 0) = 0$  and  $P'_Y(0, 0) = 0$ . The coefficients of the algebraic series  $f(X) = \sum f_n X^n$ , defined implicitly by  $f(X) = P(X, f(X))$ , have the form of an infinite sum*

$$f_n = \sum_{m \geq 1} [X^n Y^{m-1}](1 - P'_Y(X, Y))P^m(X, Y).$$

Here we prove that a generalization of the formula is a simple consequence of Proposition 1

**Theorem 5.** Let  $P(X, Y)$  be a polynomial over a field  $\kappa$  such that  $P(0, 0) = 0$  and  $P'_Y(0, 0) = 0$ . The coefficients of the algebraic series  $f(X) = \sum_{n \geq 1} f_n X^n$ , defined implicitly by  $f(X) = P(X, f(X))$ , have the form of an infinite sum

$$f_n = \sum_{m \geq 1} [X^n Y^{m-1}] (1 - P'_Y(X, Y)) P^m(X, Y).$$

*Proof.* Let the polynomial  $Q(X, Y)$  be defined as  $Q(X, Y) = P(X, Y) - Y$ , then  $Q'_Y(0, 0) = P'_Y(0, 0) - 1 \neq 0$ , and  $Q(X, f(X)) = P(X, f(X)) - f(X) = 0$ . According to Proposition 1,

$$\begin{aligned} f &= \mathcal{D}\{Y^2 \frac{\partial Q}{\partial Y}(XY, Y)/Q(XY, Y)\} \\ &= \mathcal{D}\{Y^2 (\frac{\partial P}{\partial Y}(XY, Y) - 1)/(P(XY, Y) - Y)\} \\ &= \mathcal{D}\{Y(1 - \frac{\partial P}{\partial Y}(XY, Y))/(1 - \frac{P(XY, Y)}{Y})\} \\ &= \mathcal{D}\{Y(1 - \frac{\partial P}{\partial Y}(XY, Y))(1 + \sum_{m \geq 1} (\frac{P(XY, Y)}{Y})^m)\}. \end{aligned}$$

We have the last equality due to the fact that  $P'_Y(0, 0) = 0$ ,  $\frac{P(XY, Y)}{Y}$  has no constant term, and therefore  $1/(1 - \frac{P(XY, Y)}{Y}) = 1 + \sum_{m \geq 1} (\frac{P(XY, Y)}{Y})^m$ .

As in each term of  $Y(1 - \frac{\partial P}{\partial Y}(XY, Y))$  the power of  $Y$  is larger than that of  $X$ , it cannot contribute to the diagonal. Therefore,

$$\begin{aligned} f_n &= [X^n Y^n] Y(1 - \frac{\partial P}{\partial Y}(XY, Y))(1 + \sum_{m \geq 1} (\frac{P(XY, Y)}{Y})^m) \\ &= [X^n Y^n] Y(1 - \frac{\partial P}{\partial Y}(XY, Y))(\sum_{m \geq 1} (\frac{P(XY, Y)}{Y})^m) \\ &= \sum_{m \geq 1} [X^n Y^{m-1}] (1 - \frac{\partial P(X, Y)}{\partial Y}) P^m(X, Y). \end{aligned}$$

□

### 3 $p$ -kernel of a rational fraction and Christol's Theorem

The following theorem is a generalization of Christol's Theorem in two variables:

**Theorem 6.** (Salon [8]) Let  $\mathbb{F}_q$  be a finite field of characteristic  $p$ . A formal power series

$$f = \sum_{(n_1, \dots, n_m) \in \mathbb{N}^m} u_{n_1, \dots, n_m} X_1^{n_1} \cdots X_m^{n_m} \in \mathbb{F}_q[[X_1, \dots, X_m]]$$

is algebraic over the rational function field  $\mathbb{F}_q(X_1, \dots, X_m)$  if and only if the  $p$ -kernel of  $u$

$$\{(u_{n_1 \cdot p^k + r_1, \dots, n_m \cdot p^k + r_m})_{n_1, \dots, n_m} \mid k \in \mathbb{N}, r_i = 0, 1, \dots, p^k - 1\}$$

is finite.

This theorem, whose proof does not use Theorem 1, gives another proof of the latter:

*Proof of Theorem 1.* Let  $\mathbb{F}_q$  be a finite field of characteristic  $p$ . A formal power series in  $\mathbb{F}_q[[X_1, X_m]]$

$$f(X_1, \dots, X_m) = \sum_{n_1, \dots, n_m} u_{n_1, \dots, n_m} X_1^{n_1} \dots X_m^{n_m}$$

that represents a rational functions of  $X$  and  $Y$  is algebraic over  $\mathbb{F}_q(X_1, \dots, X_m)$ . By Theorem 6, the  $p$ -kernel of the sequence  $(u_{n_1, \dots, n_m})_{n_1, \dots, n_m}$  is finite. This means that the  $p$ -kernel of its diagonal  $(u_{n, \dots, n})_n$  is finite. Thus, by Theorem 3, the power series  $\sum_n u_{n, \dots, n} X^n$  in  $\mathbb{F}_q[[X]]$  is algebraic over  $\mathbb{F}_q(X)$ .  $\square$

On the other hand, by Theorem 2 and a direct examination of the  $p$ -kernel, we can re-prove one direction of Christol's Theorem. It should be noted that Christol [3] gave a similar proof for characteristic sequences.

**Proposition 2.** *For  $P(X, Y), Q(X, Y)$  polynomials in  $\mathbb{F}_q[X, Y]$ , where  $Q(X, Y)$  has a non-zero constant term, the  $p$ -kernel of the coefficient sequence of the formal power series  $\frac{P(X, Y)}{Q(X, Y)}$  is finite.*

**Corollary 1.** *If the formal power series*

$$f = \sum_{n=0}^{\infty} u_n X^n \in \mathbb{F}_q[[X]]$$

*is algebraic over the rational function field  $\mathbb{F}_q(X)$ , the  $p$ -kernel of  $u$*

$$\{(u_{n \cdot p^k + r})_n \mid k \in \mathbb{N}, r = 0, 1, \dots, p^k - 1\}$$

*is finite.*

*Proof.* If the formal power series  $f$  is algebraic over the rational function field  $\mathbb{F}_q(X)$ , by Theorem 2,  $f$  is the diagonal of a rational function  $R(X, Y)$  in  $\mathbb{F}_q[[X, Y]]$ . By Proposition 2, the  $p$ -kernel of  $R(X, Y)$  is finite, and therefore the  $p$ -kernel of its diagonal  $f$  is finite.  $\square$

Before proving Proposition 2 we first recall an easy lemma:

**Lemma 1.** *For an element  $A$  in  $\mathbb{F}_q((X, Y))$ ,  $A = \sum_{m, n} a_{m, n} X^m Y^n$ , we let  $\Lambda_{r, s}(A)$  denote the formal power series  $\sum_{m, n} a_{mq+r, nq+s} X^m Y^n$ . Note that  $\Lambda_{r, s}$  is sometimes called a Cartier operator. For  $A, B \in \mathbb{F}_q((X, Y))$ , we have  $\Lambda_{r, s}(A^q B) = A \Lambda_{r, s}(B)$*

*Proof.* As all the coefficients are in  $\mathbb{F}_q$ , we have

$$\left( \sum_{m, n} a_{m, n} x^m y^n \right)^q = \sum_{m, n} a_{m, n}^q x^{mq} y^{nq} = \sum_{m, n} a_{m, n} x^{mq} y^{nq}$$

$$\begin{aligned} [x^m y^n] \Lambda_{r, s}(A^q B) &= [x^{mq+r} y^{nq+s}](A^q B) \\ &= \sum_{\substack{c_1+c_2=mq+r \\ c_3+c_4=nq+s}} [x^{c_1} y^{c_3}] A^q \cdot [x^{c_2} y^{c_4}] B \\ &= \sum_{\substack{qc'_1+c_2=mq+r \\ qc'_3+c_4=nq+s}} a_{c'_1 c'_3} \cdot b_{c_2 c_4} \\ &= \sum_{\substack{c'_1+c'_2=m \\ c'_3+c'_4=n}} a_{c'_1 c'_3} \cdot b_{c'_2 q+r, c'_4 q+s} \\ &= [x^m y^n](A \Lambda_{r, s}(B)). \end{aligned}$$

□

*Proof of Proposition 2.* We let  $\mathbf{\Lambda}$  denote the set of operators  $\{\Lambda_{r,s} \mid r, s \in \{0, 1, \dots, q-1\}\}$ . The  $q$ -kernel of  $\frac{P}{Q}$  is generated by  $\frac{P}{Q}$  and the operations in  $\mathbf{\Lambda}$ . Let  $\Lambda_0$  be an element in  $\mathbf{\Lambda}$ , then by the previous lemma,

$$\Lambda_0\left(\frac{P}{Q}\right) = \Lambda_0\left(\frac{PQ^{q-1}}{Q^p}\right) = \frac{\Lambda_0(PQ^{q-1})}{Q}.$$

If we let  $a$  and  $b$  denote the degree of  $P$  and  $Q$ , then

$$\deg(\Lambda_0(PQ^{q-1})) \leq \frac{a + b(q-1)}{q} < a + b.$$

Let  $P_1$  denote  $\Lambda_0(PQ^{q-1})$ . Take another element  $\Lambda_1$  in  $\mathbf{\Lambda}$ , then

$$\Lambda_1\left(\Lambda_0\left(\frac{P}{Q}\right)\right) = \Lambda_1\left(\frac{P_1}{Q}\right) = \frac{\Lambda_1(P_1Q^{q-1})}{Q}$$

$$\deg(\Lambda_1(P_1Q^{q-1})) \leq (\deg(P_1) + \deg(Q) \cdot (q-1))/q < (a + b + b \cdot (q-1))/q < a + b.$$

By induction, after applying the elements of  $\mathbf{\Lambda}$  to  $\frac{P}{Q}$ , we always get an element in the set

$$\left\{\frac{R}{Q} \mid R \in \mathbb{F}_q(X, Y), \deg(R) < a + b\right\}.$$

As the field is finite, the number of polynomials of degree less than  $a + b$  is finite and so is the  $q$ -kernel. This ends the proof as the  $p$ -kernel of a sequence is finite if and only if its  $q$ -kernel is finite.

□

## 4 Miscellaneous

### 4.1 Annihilating polynomial of algebraic functions

Theorem 2 states that if a series  $\phi(X) = \sum_{n \geq 0} u_n X^n \in \mathbb{F}_q[[X]]$  is algebraic over  $\mathbb{F}_q(X)$ , then it is the diagonal of a rational function  $R(X, Y) \in \mathbb{F}_q(X, Y)$ . The same result is proved by Fagnot [5] using combinatorial methods.

From the proof of Proposition 1 and Theorem 2 in [6] we know that  $R(X, Y)$  can be constructed from a relation of the form

$$A_0(X)\phi^{q^l}(X) + A_1(X)\phi^{q^{l+1}}(X) + \dots + A_n(X)\phi^{q^{n+l}}(X) = 0. \quad (1)$$

We now show how to obtain such a relation for a given algebraic series  $\phi(X) = \sum_{n \geq 0} u_n X^n \in \mathbb{F}_q[[X]]$ . Suppose that the sequence  $(u_n)_n$  is given. By this we mean that we know either an automaton that generates  $(u_n)_n$  or the  $q$ -kernel of  $(u_n)_n$  with initial conditions. For the definition of automata and its link with algebraic series see [4].

Let  $E = \{u^1, u^2, \dots, u^d\}$  with  $u^1 = u$  be the  $q$ -kernel of  $(u_n)_n$ .  $E$  is stable by the maps:

$$(u_n^i)_n \rightarrow (u_{qn+r}^i)_n \text{ for } r = 0, 1, \dots, p-1.$$

That is to say, there exists a map  $f$  from  $\{1, 2, \dots, d\} \times \{0, 1, \dots, p-1\}$  to  $\{1, 2, \dots, d\}$  such that

$$(u_{nq+r}^i)_n = (u_n^{f(i,r)})_n$$

Define the matrix  $A(X)$  in  $\mathbb{F}_q[X]^{d \times d}$ , where

$$A_{i,j}(X) = \sum_{\{r|f(i,r)=j\}} X^r.$$

Define the formal power series  $G_1, \dots, G_d$  by

$$G_i(X) = \sum_{n=0}^{\infty} u_n^i X^n.$$

The series can be written as

$$\begin{aligned} G_i(X) &= \sum_{r=0}^{q-1} \sum_{m=0}^{\infty} u_{qm+r}^i X^{qm+r} \\ &= \sum_{r=0}^{q-1} X^r \sum_{m=0}^{\infty} u_{qm+r}^i X^{qm}, \\ &= \sum_j A_{i,j}(X) \sum_{m=0}^{\infty} u_m^j X^{qm}, \\ &= \sum_j A_{i,j}(X) G^j(X^q). \end{aligned}$$

Writing the equalities in matrix form and using the fact that  $P(X^{q^k}) = P(X)^{q^k}$  for  $P(X)$  in  $\mathbb{F}_q[X]$  we have:

$$\begin{pmatrix} G_1(X) \\ G_2(X) \\ \vdots \\ G_d(X) \end{pmatrix} = A(X) \begin{pmatrix} G_1(X)^q \\ G_2(X)^q \\ \vdots \\ G_d(X)^q \end{pmatrix}.$$

More generally,

$$\begin{pmatrix} G_1(X)^{q^k} \\ G_2(X)^{q^k} \\ \vdots \\ G_d(X)^{q^k} \end{pmatrix} = A(X^{q^k}) \begin{pmatrix} G_1(X)^{q^{k+1}} \\ G_2(X)^{q^{k+1}} \\ \vdots \\ G_d(X)^{q^{k+1}} \end{pmatrix}.$$

And therefore for  $k \geq 1$

$$\begin{pmatrix} G_1(X) \\ G_2(X) \\ \vdots \\ G_d(X) \end{pmatrix} = \prod_{i=0}^{k-1} A(X^{q^i}) \begin{pmatrix} G_1(X)^{q^k} \\ G_2(X)^{q^k} \\ \vdots \\ G_d(X)^{q^k} \end{pmatrix}.$$

Denoting the  $i$ -th row of a matrix  $M$  by  $M_i$ , we have

$$\begin{pmatrix} G_1(X) \\ G_1(X)^q \\ \vdots \\ G_1(X)^{q^d} \end{pmatrix} = \begin{pmatrix} (\prod_{i=0}^d A(X^{q^i}))_1 \\ (\prod_{i=1}^d A(X^{q^i}))_1 \\ \vdots \\ (\prod_{i=d}^d A(X^{q^i}))_1 \end{pmatrix} \begin{pmatrix} G_1(X)^{q^{d+1}} \\ G_2(X)^{q^{d+1}} \\ \vdots \\ G_d(X)^{q^{d+1}} \end{pmatrix}.$$

This equality is of the form

$$\begin{pmatrix} G_1(X) \\ G_1(X)^q \\ \vdots \\ G_1(X)^{q^d} \end{pmatrix} = B(X) \cdot \begin{pmatrix} G_1(X)^{q^{d+1}} \\ G_2(X)^{q^{d+1}} \\ \vdots \\ G_d(X)^{q^{d+1}} \end{pmatrix},$$

where  $B(X)$  is a matrix in  $\mathbb{F}_q(X)^{(d+1) \times d}$ . There exists a linear combination of the  $d+1$  rows of  $B(X)$  that is equal to 0. This means that the linear combination of  $G_1(X), \dots, G_d(X)^{q^d}$  with the same coefficients is 0, which is a relation of the form (1).

## 4.2 Formal power series solutions of polynomials

The main result of this article (Theorem 5) allows us to calculate the coefficients of an algebraic series using an annihilating polynomial of it, when the latter satisfies certain conditions. For a formal power series in  $\mathbb{F}_q[[X]]$  that is algebraic over  $\mathbb{F}_q(X)$ , we can calculate its coefficients in a simpler way by knowing an automaton that generates them. We have shown how to find an annihilating polynomial of an algebraic function in the previous subsection. Now we start from a polynomial in  $\mathbb{F}_q(X)[Y]$  and show how to find automata that generate its roots in  $\mathbb{F}[[X]]$  with typical examples.

**Example 1.**  $P(X, Y) = (1 + X)^3 Y^2 + (1 + X)^2 Y + X \in \mathbb{F}_2[X, Y]$ . There exists  $f(X) \in \mathbb{F}_2[[X]]$  such that  $P(X, f(X)) = 0$ . This is because  $P(X, \sum_{n \geq 0} a_n X^n) = 0$  if and only if  $(a_n)$  satisfies the condition

$$[x^n]P(X, \sum_{n \geq 0} a_n X^n) = 0, \text{ for all } n \in \mathbb{N}.$$

The first two equations are  $a_0 + a_0 = 0$  and  $a_0 + a_1 + 1 = 0$ . And for  $n \geq 2$ ,  $a_n$  appears for the first time in the  $n$ -th equation. As we have a new variable for every constraint except for the first two equations, there exist two solutions, which correspond to  $a_0 = 0$  and  $a_0 = 1$ .

Let  $f$  be a solution of  $P(X, f(X)) = 0$ ,  $f$  has degree 2 over  $\mathbb{F}_q(X)$ , therefore  $f$ ,  $f^2$  and  $f^4$  are linearly dependent over  $\mathbb{F}_q(X)$ . A relation can be found by writing them all as linear combinations of 1 and  $f$ . That is,

$$\begin{aligned}
f^2 &= \frac{X}{(1+X)^3} + \frac{1}{1+X}f \\
f^4 &= (f^2)^2 \\
&= \frac{X^2}{(1+X)^6} + \frac{1}{(1+X)^2}f^2 \\
&= \frac{X^2}{(1+X)^6} + \frac{1}{(1+X)^2} \left( \frac{X}{(1+X)^3} + \frac{1}{1+X}f \right) \\
&= \frac{X}{(1+X)^6} + \frac{1}{(1+X)^3}f
\end{aligned}$$

Therefore,

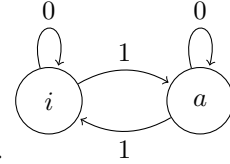
$$f^4 + \frac{1}{(1+X)^3}f^2 + \frac{X}{(1+X)^4}f = 0.$$

We apply the Cartier operators  $\Lambda_0$  and  $\Lambda_1$  repetitively to

$$f = \frac{(1+X)^4}{X}f^4 + \frac{1+X}{X}f^2.$$

We have

$$\begin{aligned}
\Lambda_0(f) &= f \\
\Lambda_1(f) &= \frac{f^2}{x} + xf^2 + \frac{f}{x} =: f_1 \\
\Lambda_0(f_1) &= f_1 \\
\Lambda_1(f_1) &= f.
\end{aligned}$$



Therefore  $f$  is generated by the automaton below with initial state  $i$ :

There are four sequences that can be defined by this automaton, and the only two that satisfy the condition  $a_0 + a_1 = 1 = 0$  are the sequences that correspond to the maps

$$\pi_1(i) = 0$$

$$\pi_1(a) = 1,$$

and

$$\pi_2(i) = 1$$

$$\pi_2(a) = 0.$$

These two sequences are the solutions of  $P(X, f(X)) = 0$ , because we know from the beginning of the example that the equation  $P(X, f(X)) = 0$  has exactly two solutions in  $\mathbb{F}_q[X]$ , and each solution is defined by the automaton above. These two sequences are the Thue-Morse sequence and its bitwise negation.



**Example 2.**  $Q(X, Y) = Y^2 + (1 + X)Y + X^2 \in \mathbb{F}_2[X, Y]$ . It can be shown with the same argument as for the first example, that the equation  $Q(X, f(X)) = 0$  has two solutions in  $\mathbb{F}_q[X]$ .

Writing  $f$ ,  $f^2$  and  $f^4$  as linear combinations of 1 and  $f$  over  $\mathbb{F}_q(X)$ , we find the relation

$$f^4 + f^2 + (X^2 + X^3)f = 0.$$

Applying  $\Lambda_0$  and  $\Lambda_1$  repetitively to

$$f = \frac{f^4}{X^2 + X^3} + \frac{f^2}{X^2 + X^3}$$

we get

$$\Lambda_0(f) = \frac{f^2}{X(1+X)} + \frac{f}{X(1+X)} =: f_1$$

$$\Lambda_1(f) = f_1$$

$$\Lambda_0(f_1) = \frac{f}{1+X} =: f_2$$

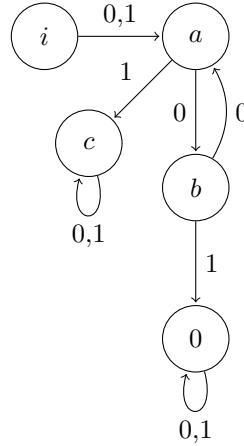
$$\Lambda_1(f_1) = \frac{f^2}{X^2(1+X)} + \frac{f}{X^2} =: f_3$$

$$\Lambda_0(f_2) = f_1$$

$$\Lambda_1(f_2) = 0$$

$$\Lambda_0(f_3) = A_1(f_3) = f_3.$$

Therefore  $f$  can be generated by the automaton below with initial state  $i$ :



The equation  $[X^1]Q(X, f(X)) = 0$  gives  $a_0 = a_1$ , and the equation  $[X^2]Q(X, f(X)) = 0$  gives  $a_2 = 1$ . The sequences that satisfy these two conditions are defined by this automaton with the map

$$\pi_1(i) = \pi_1(a) = 0$$

$$\pi_1(c) = 1$$

$$\pi_1(0) = 0$$

or

$$\pi_2(i) = \pi_2(a) = 1$$

$$\pi_2(c) = 1$$

$$\pi_2(0) = 0.$$

These two sequences are the two solutions of  $Q(X, f(X)) = 0$  in  $\mathbb{F}_q[X]$ .

## References

- [1] B. Adamczewski and J. P. Bell, “Diagonalization and rationalization of algebraic Laurent series”, *Ann. Sci. Éc. Norm. Supér.* 46 (2013), 963–1004
- [2] C. Banderier and M. Drmota, “Coefficients of algebraic functions: formulae and asymptotics”, *FPSAC 2013 Paris, France DMTCS proc. AS*, 2013, 1095–1106.
- [3] G. Christol, “Ensembles presque périodiques k-reconnaissables”, *Theoretical Computer Science*, t. 9, 1979, p. 141–145.
- [4] G. Christol, T. Kamae, M. Mendès France and G. Rauzy, “Suites algébriques, automates et substitutions”, *Bull. Soc. Math. France*, 108, 1980, p 401–419.
- [5] I. Fagnot, “Łukasiewicz language and diagonals of formal series”, *J. Théor. Nombres Bordeaux*. 8 (1996), no. 1, 31–46.
- [6] H. Furstenberg, “Algebraic functions over finite fields”, *J. Algebra* 7, 271–277 (1967).
- [7] P. Lairez, “Périodes d’intégrales rationnelles, algorithmes et applications”, Thèse de doctorat, École Polytechnique (2014). Available at the URL <https://pastel.archives-ouvertes.fr/tel-01089130/document>
- [8] O. Salon, “Suites automatiques à multi-indices”, *Séminaire de Théorie des Nombres de Bordeaux*, exposé no.4 (1986-1987), 4.01–4.36. Available at the URL <http://resolver.sub.uni-goettingen.de/purl?GDZPPN002545691>
- [9] A. D. Sokal, “A ridiculously simple and explicit implicit function theorem”, *Sém. Lothar. Combin.* 61A (2009/10), Art. B61Ad, 21 pp.
- [10] M. Soria, Thèse d’habilitation (1990), LRI, Orsay.